Categorization and Assessment of Models of VSSS in the Context of Communication

Ali Mohammad Norouzzadeh

***Abstract*— Video transmission is a key technology of security monitoring systems used in communication platform. Considering the nearly indestructible architecture of a video surveillance system as introduced in "NIVSS: A Nearly Indestructible Video Surveillance System". Surveillance is defined as the close observation and monitoring of changing information. Evaluation of the proposed methods in this area shows a variety of approaches. On the one hand, such a variety of video security surveillance system models and the lack of a coherent framework for them on the other hand have foreclosed the possibility of comparing and evaluating methods from researchers. Accordingly in this paper, in addition to propose a coherent framework for models, we proceed to identify them and their challenges that can lead to a more precise understanding of these models and the accurate and systematic use of them.**

***Index Terms*— component; Video Security Surveillance System; Video Surveillance System; models based VSSS, Video Surveillance**

I. INTRODUCTION

Due to social security is becoming increasingly serious, we needs a large number of security personnel to do the works of security every year. Now, monitoring some places (such as senior residential community, commercial buildings, parking lot, et al) gets mainly through the arrangement of the security staff and video monitoring equipment. However, these measures can't meet the security requirements, which are becoming increasingly serious. The security management is responsible for the security management process and follows the three main security principles which are availability, confidentiality and integrity. Other responsibilities include risk assessment and analysis which result in security policies, information classification and security-awareness training of the personnel [1]. On the one hand, in the high-intensity work environment, some people might occur omissions because the energy and attention is limited; on the other hand, the traditional video surveillance system has only monitoring and storage function, and thus can't timely response to the abnormal situation [3]. It is a challenging problem since no technology can provide satisfactory performance up to now in the state of art of video security surveillance system [5]. Figure1 show the structure of video surveillance system that based on C / S (Client / Server) mode, including front-end monitoring point and back-end monitoring point [8]. So video surveillance system recognizes, keeps track of security threats of the real environment which threatens personal safety, and protects the individual from them with visual devices gathering video information such as CCTVs and IP cameras.

In this paper, in addition to proposing a coherent framework for these approaches based Video Security Surveillance System (VSSS) in the context of communication, we proceed to identify and introduce these approaches and their challenges, which can lead to a more precise understanding of them and the accurate and systematic use of them based on need. The rest of the paper is organized as follows: section 2, In addition to providing a review of related works, introduces several proposed definitions for VSSS. Section 3 identifies and offers the most important approaches VSSS. Section 4 presents the results of this study and future work.

II. RELATED WORK

In a public environment, due to the low public acceptance of video surveillance especially [9] special care has to be taken by security management to avoid image loss, protests and legal actions. This topic is especially relevant for places that are not normally seen as critical infrastructure like transportation hubs or government buildings. As an example of an action, which needs to be noted as "non-technical" security take the case of Austria, where each closed-circuit television (CCTV) installation which allows the collection of individual-related information has to be reported to the "Datenschutzkommission" (DSK) [17].

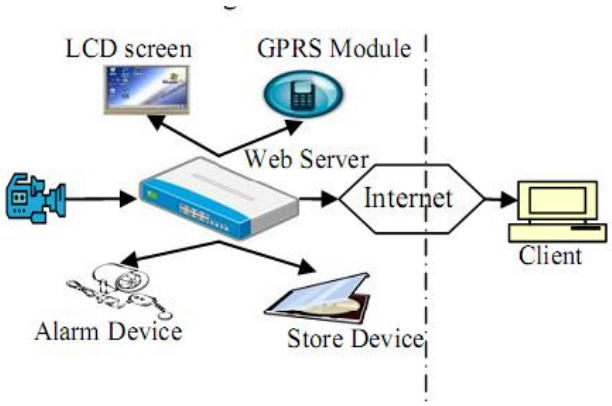

Figure1. The structure of video surveillance system based on C / S (Client / Server) mode

DSK then weights the privacy concerns to the proposed security benefit; in the case of public low risk buildings permission is seldom given or with strict obligations. The

Manuscript received July 20, 2014.
Ali Mohammad Norouzzadeh, Islamic Azad University, Qazvin, Iran.

architecture of the security management process with a focus on a video surveillance system as well as a more detailed view of these topics is shown in figure 2. As can be seen, the main aspects of the security management process are physical security, operation security, application security, network security and access control. Each of these aspects represents a topic which can be broken into several subtopics that further increases the modularity.

The physical security aspect of the security management process is responsible to prevent or deter intruders from accessing a facility and to deny attackers the illegal usage of resource or information stored on any type of media. For a video surveillance system one should note that physical security needs to be treated from two different angles: On the one hand it provides part of a physical security strategy including analysis of possible locations for check points and authorization equipment as well as determining a well-defined site periphery that minimizes the possible attack routes and entry points of intruders. On the other hand physical security for the CCTV system needs to be provided which encompasses the protection of site critical infrastructure e.g. power lines or network wires or server equipment from vandalism [1].

Network security management provides policies, procedures and guidelines in order to prevent electronic attacks from the inside and outside on protocols and equipment endangering the integrity, confidentiality and accountability of the information transported in the network without hindering of allowed communication. In a CCTV system this is especially true because of the requirement to transfer a large number video streams simultaneously and store the same in some kind of storage network. Network security also deals with the management of the capacities of the office and security relevant network infrastructure: higher levels of traffic in the office network must not compromise the quality of performance of the security network. However if the security network is on its limits, parts of the data could be rerouted through the office network to ensure a fully functional video surveillance system. Of course proper actions must be taken to protect the security of the data transferred. Network security management has to make sure that all requirements of that end find their way into the Security Management documentation so that the types of networks as well as the principal failover mechanism are described in a technology independent way.

Access control is the ability to permit or deny the use of a particular resource which includes physical and software resources by a particular entity. In a video surveillance system access control is a major factor for the video and metadata streams because of the sensitive nature of the data transferred; this means that an identity management system has to be implemented which is responsible for the authentication of users and the privileges they are granted. This authentication process is normally dependent on the physical security and the hardware provided but can also be implemented using a purely software based approach which falls into the department of application security.

Operational security deals with all processes needed to operate the video surveillance system. As we are looking at a highly distributed system, the analysis of all processes will be somewhat complex. On the pure IT side one major point is to administrate and configure the video surveillance system. Subtopics include the backup management of video streams, metadata and access logs which policies need to be corresponding to the legal obligations regarding the storage of the before mentioned data. This management process also Subtopics include the backup management of video streams, metadata and access logs which policies need to be corresponding to the legal obligations regarding the storage of the before mentioned data. This management process also includes the elaboration of workflows regarding the updates of the video analysis, accounting both software and configuration updates. Furthermore the interval of more elaborate system health checks used to ensure the system integrity and the absence of sensory tampering.

Application security encompasses measures taken to prevent exceptions in the security policy through flaws in the design, development, or deployment of the application. In the context of CCTV this means that the software and any sub-sequential updates have to comply to information and quality management standards like ISO/IEC FDIS 27001 [2] and ISO 9000. In addition predefined test cases are used to determine the required performance including false positive and true positive rates or resource ratios that have to be met.

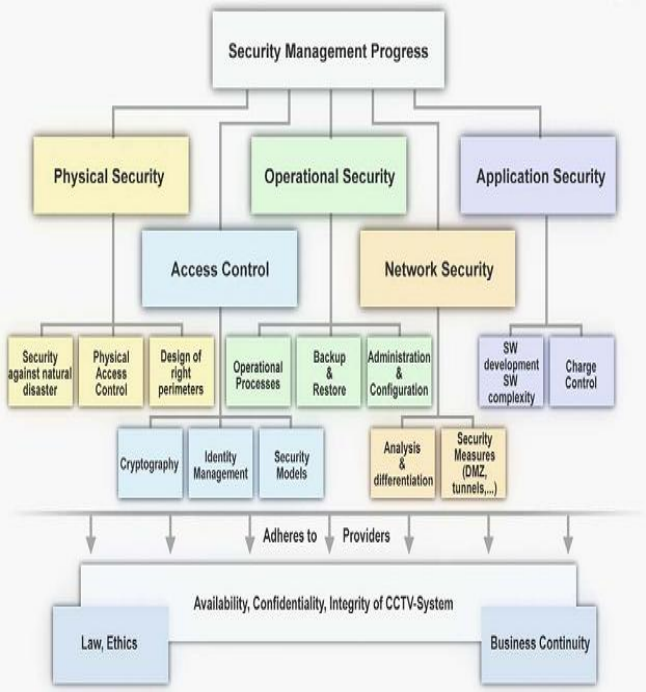

Figure2. Hierarchy structure of Security in the Video Surveillance System (VSS)

III. PROPOSED FRAMEWORK

Recently, automatic video surveillance technology emerges as an important component of security system since manual video surveillance is usually a labor-intensive task and error prone [5]. Increasing needs in security drive many areas to deploy a large number of cameras, but many systems of manual monitoring is a rather tedious task and it is easy for

security person to loose his attention [16]. The safety in a specified space can be monitored and secured by an automatic video security system to prevent the abnormality in people's movement and behavior, and unauthorized access to restricted areas [6], [7]. Automation video security technology can help overcome the problems of manual systems in terms of cost and performance issues. It allows security people to free from labor-intensive tedious tasks, and to concentrate on more effective intelligent tasks. The capability of normalcy decision in a security system is one of the most important and difficult task. This paper discusses the models of VSSS. At the rest of the section, these two models and their approaches are presented separately. Figure 3. Show a coherent framework for VSSS that can lead to a more precise understanding of these models and the accurate and systematic use of them.

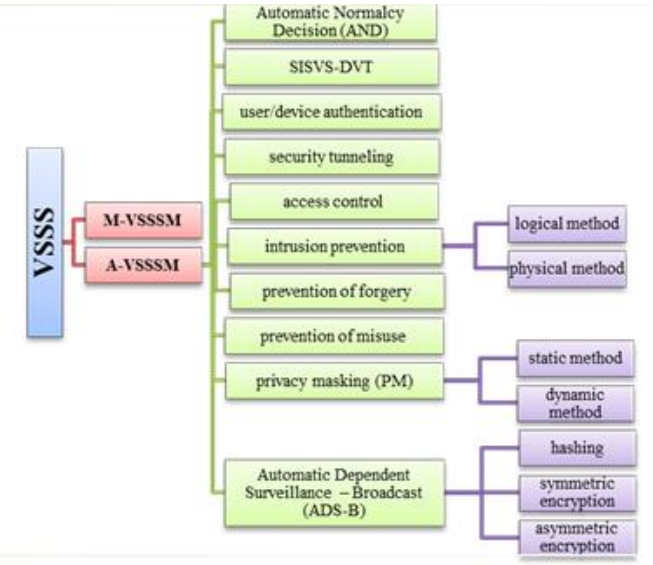

Figure 3. Coherent framework for VSSS

A. Manual VSSS Model(M-VSSSM)

Manual video surveillance is usually a labor-intensive task and error-prone. Increasing needs in security drive many areas to deploy a large number of cameras, but many systems of manual monitoring is a rather tedious task and it is easy for security person to loose his attention. The safety in a specified space can be monitored and secured by an automatic video security system to prevent the abnormality in people's movement and behavior, and unauthorized access to restricted areas. So automatic video surveillance technology emerges as an important component of security system.

B. Automated VSSS Model(A-VSSSM)

There are immediate needs for automated surveillance systems in commercial, law enforcement, and military applications [14], [15]. Security strength of the design alternatives is determined from research. Feasibility criteria are determined by comparative analysis of alternatives. Economic implications and possible collision risk is determined from simulations that model the United State airspace over the Gulf of Mexico and part of the airspace under attack respectively. This model can be divided into ten categories. At the rest of the section discussed.

1) Automatic Normalcy Decision (AND)

It is a challenging problem since no technology can provide satisfactory performance up to now in the state of art of video security surveillance system, especially in automatic normalcy decision. The implementation of the intelligent security using the framework of video surveillance needs people detection, tracking, and normalcy decision. This paper focuses on the autonomous normalcy decision after people detection and tracking have been carried out. Computer vision techniques are used to analyze video streams of multiple people movements acquired from multiple video cameras [17] developed by GE GRC's (GE Global Research Center). The extracted trajectories from people movements are used to construct trajectory ontology, and to monitor and produce alarm based on trajectory ontology. The system works incremental way by adapting itself toward both varying environments, and provides interactive interface with changing security strategy. The ontology constructor has three ontological clusters in the first level of the ontological tree, and the three ontological clusters are the clusters of "Forward movement", "T-turn", and "Wondering". The cluster of the forward movement is
split into "Suspicious forward movement" and "Normal forward movement" in the 2nd level of the ontological tree [11]. Figure 4. show historical ontology.

2) Automatic Dependent Surveillance – Broadcast (ADS-B)

ADS-B is dependent on digital communications between aircraft and ground stations of the air route traffic control center (ARTCC); however these communications are not secured. Anyone with the appropriate capabilities and equipment can interrogate the signal and transmit their own false data; this is known as spoofing. The possibility of this type of attacks decreases the situational awareness of United States airspace [10]. Three alternative methods of securing ADS-B signals are evaluated: hashing, symmetric encryption, and asymmetric encryption.

a) Hashing

The primary goal of hashing is to confirm the identity of the source of a message. This is achieved by creating a hash that is attached at the end of the message. A hash is a digest of a message created by running a hashing algorithm by the sender. This digest is verified at the receiver's station by running the same algorithm and deriving the hash independently. The computer at the receiver's station then compares the received digest to the independently derived digest. If both of them are identical, then the message can be considered authentic.
Hashing algorithms run very quickly and only require a software upgrade. However, it will require usage of additional bits in ADS-B message that are fully used right

now. A possible compromise would be to free any 8 bits that are currently being used.

b) Symmetric Encryption

Encryption is the conversion of plain text to cipher text by implementing various algorithms. Running an encryption algorithm on a message will scramble it and make it look illegible. However, if the receiver knows the right algorithm and key, the message can be decrypted. A key is used to encrypt and decrypt messages. The main goals of encryption are ensuring confidentiality, non-repudiation, authenticity, and integrity. Confidentiality insures that only the sender and the intended recipient can see the message. Non-repudiation is the ability of the encryption algorithm to provide proof of the message's source. Authenticity confirms the identity of the sender. Integrity refers to the content of the message and the accuracy of the information sent in the message [12]. For symmetric encryption, each entity has a secret key and uses this key to encrypt ADS-B messages. The receiving entities also have access to these keys and use the keys to decrypt the message. Symmetric encryption relies on the strength of the key and the reliability of the key exchange process. A strong symmetric encryption will have a long key as well as a secure system for key exchanges. The implementation of symmetric encryption will require software upgrade with no additional hardware [10].

c) Asymmetric Encryption

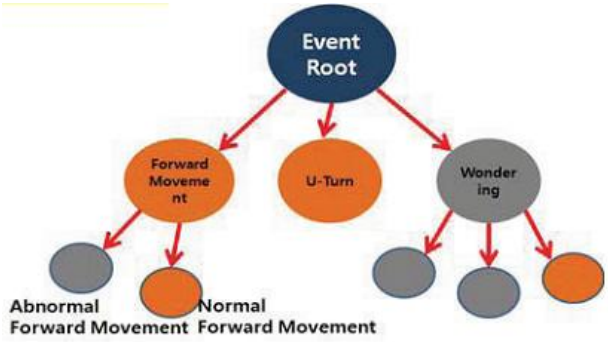

Figure 4. example for ontology in the AND

Asymmetric encryption is very similar to symmetric. However, asymmetric encryption entitles each entity to two keys–private and public. The public key is known to everyone while the private key is only known to a particular entity. Both keys are mathematically dependent on each other. The message that is being sent from entity A is being encoded by the private key of A, and then encoded again with the public key of receiving entity B. Then, the message is being transmitted through public space until entity B receives it. Entity B will then decode the message by using its private key first and then decode it by using A's public key. The decrypted message is then received at B. Asymmetric encryption does not have the security issue of key exchanges like the symmetric encryption, but this alternative still has to have a way to share all public keys between entities. This alternative will also require knowing the recipient before sending the message, similar to secondary radar, which might degrade the positive factors of ADS-B real time location data [10].

3) DaVinci technology

A system of intelligent security video surveillance based on DaVinci technology (SISVS-DVT) uses some algorithms, including the moving target detection and tracking, face detection and recognition, image compression and other related algorithms; apply the background subtraction, the Kalman filter, the Adaboost, the PCA (Principal Component Analysis), JPEG, and other algorithms to the video surveillance system; built a hardware platform based on DaVinci technology, which has dual-core processor architecture whose fast computing capability and efficient control enable the system to have a better real-time; design the embedded Web server based on the hardware platform; develop the functional modules, including the moving object detection, face detection and recognition, and GPRS MMS Transceiver. In order to minimize losses and gain first-hand evidence, customers can timely access to the surveillance images via phone or Internet by using the system; on the same time, it reduces the required human, material and financial resources to hire a large number of security personnel [4].

4) PrivacyMasking(PM)

As video information gathered by multiple IP cameras includes people, vehicles, space information of private lives and other privacy-sensitive information, an appropriate technology that protects the privacy-sensitive information and prevents illegal exposure is needed [13]. PM technology is categorized into static method and dynamic method. The static privacy masking method protects fixing ROIs (Region of Interest) like windows. On the other hands, the dynamic privacy masking method is used to protect mobile ROIs including people, moving vehicles.

5) User/Device Authentication

As video information gathering devices, video storage devices, video controllers, and video service providers consisting video surveillance system operate based on public network, the trustable communication channels among them should primarily be considered. In addition to, a secure authentication method for authenticating user for accessing system is also needed.

6) Security Tunneling

Video information transmitted over public network is inevitably exposed to unauthorized accesses. To resolve the problems caused by unauthorized disclosure, trustable channel between communicating entities should be established, and encrypted video information should be exchanged based on it.

7) Access Contorol

Even through an administrator is involved in the privileged group that is permitted to maintain and control video information, each is desirable to be granted a different access right. It ensures safety of video information and reliable enforcement.

8) Intrusion Prevention

The intrusion prevention technology providing real-time intrusion detection and response is mandatory for protecting video information form internal/external illegal access trial, and preventing privacy infringement. The intrusion

prevention technology for video surveillance system can be categorized into logical method and physical method . The logical intrusion prevention method protects system resource from attacks using legacy IP-based network. The physical intrusion prevention method protects system resource from physical illegal access.

9) Prevention of Misuse

This security function detects the forgery of video information makes it possible to take an appropriate response.

10) Prevention of Misuse

The gathered video information involves lots of significant information. It means that if it is misused in wrong applications, it can result in unexpected damages.

IV. CONCLUSION

In this paper, the concept of VSSS as one of the most important issues in the present era has been introduced. Then, different methods and definitions provided by researchers to VSSS were expressed. Afterwards, based on these definitions and methods, a coherent framework for these approaches was identified and introduced. So, we create an appropriate context for studying, evaluating and analyzing each of the approaches. As a result, providing the possibility of consistent and correct use of VSSS based on needs. But it should be noticed that the proposed criteria pay to relations between approaches, the operations complexity and the techniques used for every approach, and also we have not presented and evaluated of VSSS. Therefore the continuation of this research is possible through definition and application of the criteria which consider mentioned cases, and evaluation a coherent framework for VSSS models.

REFERENCE

[1] K. Kraus., O. Martikainen., R. Reda., "Security Management Process for Video Surveillance Systems in Heterogeneous Communication Networks," IEEE, 978-1-4244-2829, 2008.

[2] "ISO/IEC FDIS 27001 "Information technology — Security techniques Information security management systems — Requirements" Final Draft 2005.

[3] WANG Shan. The situation and future development trend of video surveillance market in China. TELCOM WORLD,2009(9):44.

[4] Cui Baoxia, Cui Junjie,Duan Yong, "Intelligent security video surveillance system based on DaVinci technology," 2013 Fifth Conference on Measuring Technology and Mechatronics Automation. P:255-658,IEEE,2013.

[5] MiYoung Nam, HakChul Shin, YongZhe Xu and PhillKyu Rhee, Member, IEEE, "An Adaptive Normalcy Decision for Video Surveillance Security System," 2011 IEEE International Conference on Consumer Electronics (ICCE), pp:733-734, 2011.

[6] G. L. Foresti, C. S. Regazzoni, and P. K. Varshney, "Multisensor Surveillance Systems," The Fusion Perspective. Norwell, MA: Kluwer, 2003.

[7] G. L. Foresti, P. Mahonen, and C. S. Regazzoni, "Multimedia Video Based Surveillance Systems," From User Requirements to Research Solutions. Norwell, MA: Kluwer, 2000.

[8] WANG Ya-hui, CHI Xue-fen, ZHOU Ren-gui et al. Key Technology Study and Design of Embedded Real-Time Video Communication System[J]. Journal of Jilin University: Information Science Edition, 2006, 24(3): 241-246.

[9] Bowyer, K.W., Face recognition technology: security versus privacy: Technology and Society Magazine, IEEE Volume 23, Issue 1 2004.

[10] Sahar Amin, Tyler Clark, Rennix Offutt, and Kate Serenko, "Design of a Cyber Security Framework for ADS-B Based Surveillance Systems," IEEE, pp:304-309,

[11] Karoui, L.: "Intelligent Ontology Learning based on Context: Answering Crucial Questions". To appear in the IEEE International Conference on Computational Intelligence for Modelling, Control and Automation - CIMCA06, Sydney, 2006.

[12] Skalski-Pay, Jennifer, Applied Encryption: Ensuring Integrity of Tactical Data ,SANS Institute InfoSec Reading Room, 2003.

[13] Geo-Woo Kim, Jong-Wook Han, " Security model for video surveillance system," IEEE, pp: 100-104, 2012.

[14] Robert T. Collins, Alan J. Lipton, and Takeo Kanade, "Introduction to the Special Section on Video Surveillance," IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, VOL. 22, NO. 8, AUGUST 2000.

[15] Lipton, Alan, et al. A system for video surveillance and monitoring. Vol. 2. Pittsburg: Carnegie Mellon University, the Robotics Institute, 2000.

[16] Seeley, John E., and William R. Vogt. "Advanced video security system." U.S. Patent No. 6,069,655. 30 May 2000.

[17] Diaz, Luis G. Ramirez, Pedro L. Cruz Burgos, and Dan F. Rodriquez. "Video monitoring and security system." U.S. Patent No. 6,476,858. 5 Nov. 2002.

[18] Shiota, Tsuneo, and Soji Takeuchi. "Video surveillance system for selectively selecting processing and displaying the outputs of a plurality of TV cameras." U.S. Patent No. 4,943,854. 24 Jul. 1990